

REMARKS/ARGUMENTS

1.) Claim Rejections – 35 U.S.C. § 101

Claims 10 and 11 stand rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

The Examiner rejected claims 10-11 under 35 U.S.C. §101. According to the Examiner on Page 2 of the Office Action:

Applicant's arguments filed June 5, 2007 have been fully considered, at least under 35 U.S.C. 101, but they are not persuasive. ***Although the claims 10 and 11 are now statutory, the specification is still not met the 35 U.S.C. 101 condition.*** The specification recites "The instructions may be program code means loaded in a memory, such as a RAM, from a storage medium OR from another computer via a computer network, which clearly including intangible media such as signals, carrier waves, transmissions, optical waves, transmission media or other media incapable of being touched or perceived absent the tangible medium through which they are conveyed. ***Therefore, claims 10 and 11 recite a non-statutory subject matter.*** (emphasis added)

Applicant respectfully traverses the rejection. The Examiner first states that claims 10 and 11 are statutory. The Examiner then states that ***the Specification*** does not meet the 35 U.S.C. §101 condition. From that premise, the Examiner concludes that claims 10 and 11 are non-statutory. However, it is well known that ***the claims*** define the scope of the claimed invention. Paragraph 7.05.01 of the MPEP provides guidance for rejecting claims based on 35 U.S.C. §101 (emphasis added):

...the ***claimed invention*** is directed to non-statutory subject matter because [1]

Examiner Note

In bracket 1, explain why the ***claimed invention*** is not patent eligible subject matter, e.g.,

(a) why the ***claimed invention*** does not fall within at least one of the four categories of patent eligible subject matter recited in 35 U.S.C. 101 (process, machine, manufacture, or composition of matter); or

(b) why the ***claimed invention*** is directed to a judicial exception to 35 U.S.C. 101 (i.e., an abstract idea, natural phenomenon, or law of

nature) and is not directed to a practical application of such judicial exception (e.g., because the **claim** does not require any physical transformation and the invention as claimed does not produce a useful, concrete, and tangible result); or

(c) why the **claimed invention** would impermissibly cover every substantial practical application of, and thereby preempt all use of, an abstract idea, natural phenomenon, or law of nature.

Nowhere in claims 10 or 11 does the Applicant claim as part of his invention the elements ascribed thereto by the Examiner (signals, carrier waves, transmissions, optical waves, transmission media or other media incapable of being touched or perceived):

10. A computer program product embodied on a computer readable medium adapted to configure a processor to process a message to determine a tag value from the message and from a key according to a message authentication code, the computer program product comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code further comprising:

computer readable program code adapted to configure the processor to select one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and

computer readable program code adapted to configure the processor to determine the tag value to be the selected symbol.

11. A computer program product embodied on a computer readable medium adapted to configure a processor to communicate data messages, the computer program product comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code further comprising:

computer readable program code adapted to configure the processor to determine a tag value from a message and from a key according to a message authentication code;

computer readable program code adapted to configure the processor to select one of a plurality of symbols, the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and

computer readable program code adapted to configure the processor to determine the tag value to be the selected symbol.

The Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility ("Guidelines"), Section 2106 of the MPEP provides, in pertinent part, as follows (emphasis added):

II. DETERMINE WHAT APPLICANT HAS INVENTED AND IS SEEKING TO PATENT

It is essential that patent applicants obtain a prompt yet complete examination of their applications. Under the principles of compact prosecution, ***each claim should be reviewed for compliance with every statutory requirement for patentability*** in the initial review of the application, even if one or more claims are found to be deficient with respect to some statutory requirement. Thus, USPTO personnel should state all reasons and bases for rejecting claims in the first Office action. Deficiencies should be explained clearly, particularly when they serve as a basis for a rejection. Whenever practicable, USPTO personnel should indicate how rejections may be overcome and how problems may be resolved. A failure to follow this approach can lead to unnecessary delays in the prosecution of the application.

C. Review the Claims

The claims define the property rights provided by a patent, and thus require careful scrutiny. ***The goal of claim analysis is to identify the boundaries of the protection*** sought by the applicant and to understand how the claims relate to and define what the applicant has indicated is the invention. USPTO personnel must first determine the scope of a claim by thoroughly analyzing the language of the claim before determining if the claim complies with each statutory requirement for patentability. See *In re Hiniker Co.*, 150 F.3d 1362, 1369, 47 USPQ2d 1523, 1529 (Fed. Cir. 1998) ("[T]he name of the game is the claim.").

USPTO personnel should begin claim analysis by identifying and evaluating each claim limitation. For processes, the claim limitations will define steps or acts to be performed. For products, the claim limitations will define discrete physical structures or materials. Product claims are claims that are directed to either machines, manufactures or compositions of matter.

USPTO personnel are to correlate each claim limitation to all portions of the disclosure that describe the claim limitation. This is to be

done in all cases, regardless of whether the claimed invention is defined using means or step plus function language. The correlation step will ensure that USPTO personnel correctly interpret each claim limitation.

As noted, the Examiner states that **the Specification** does not meet the 35 U.S.C. §101 condition. Notably, the Applicant does not even refer to these supposedly claimed non-statutory claim elements. Rather, the Examiner first **implies** non-statutory claim elements into the Specification, and then reads these claim elements into claims 10 and 11, so as to reject the present application.

Applicant is unaware of a requirement that a Specification be silent as material that is non-statutory subject matter, lest it be incorporated into the claims. In fact, many issued patents **expressly** describe within the Specification, **but do not claim**, signals, mathematical algorithms, laws of nature, etc., in order to provide the public with a fuller understanding of the claimed invention. Applicant does not believe that a patent whose Specification refers to, or can be implied to refer to, e.g., how an apparatus processes a signal, is subject to invalidation because the claims thereof must be interpreted as incorporating the non-statutory claim element of the signal itself (as part of the apparatus). If such were the case, any patent on a wireless or computer related apparatus, all of which process signals, would be invalid, even though the signal itself is not expressly claimed.

Applicant respectfully submits that the Examiner has incorrectly asserted that a Specification (as opposed to the claims) must meet the requirements of 35 U.S.C. §101, and further, has impermissibly fashioned additional material as being implied in the Specification, and then has impermissibly deemed such fashioned material as being incorporated from the Specification as claim elements of claims 10 and 11. Hence, favorable reconsideration of claims 10 and 11 is respectfully requested in view of the foregoing remarks.

2.) Claim Rejections – 35 U.S.C. § 103(a)

Claims 1-5, 7-12 are rejected under 35 U.S.C.103(a) as being unpatentable over Graveman (US 6,851,052 81), and further in view of Carman et al (US 6,845,449 81). The Applicant respectfully traverses the rejection as it is technically impossible to

combine these two references to obtain the present invention. Because of this technical inability (as described below) to combine the two, it would not have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Graveman with the teaching of Carman to authenticate the source and integrity of transmitted or stored information. Further, the ordinary skilled person would not have been motivated to modify Graveman with the teaching of Carman to provide absolute authentication of the source or origin of a received message so as to permit verifying approximate integrity between the original message and the received message.

Graveman discloses "approximated message authentication codes" (AMAC) using the following encoding method:

1. Arrange the message bits in a matrix with A columns and T^2 rows;
 2. Permute the message bits using a suitable secret key dependent pseudo random function;
 3. Encrypt the permuted message bits using a secret key;
 4. Apply a bit majority function on T rows which results in a new A x T matrix;
- and
5. Apply the same majority function of step 4 on the A x T matrix which results in the AMAC function according to the invention of Graveman.

The foregoing is inapplicable to the present invention. In the present invention, a method based on code words from an "error correcting code" is disclosed. The matrix arrangement of Graveman is not directed to error correcting codes and the method of Graveman cannot be used with an error correcting code as such a code does not have the properties Graveman requires so as to construct a secure AMAC according to that method. In the present invention, a method is claimed where the message authentication code is based on selecting "one of a plurality of code symbols" while Graveman teaches a method that is based on taking a majority function on different specific chosen sets of bits of the original permuted and encrypted message. Graveman teaches a method where the secret key is used to *permute* the plain text message bits and then encrypt the permuted message prior to applying a majority function on the resulted new message. This is a very different use of the key compared to using the key to determine which of a plurality of code symbols to use for encoding

the message. In particular, *no encryption step* at all is performed in the present invention.

Carman is only tangentially related to the present invention as it discuss error-correcting codes. Error-correcting codes and different aspects and encoding methods have been very extensively studied in academic research and industry.

Specifically, Carman teaches a method to detect and correct errors by using an authentication mechanism that uses a reversible inner function. Besides the message and the authentication tag, the encrypted inner result is also sent as seen in Figure 15 and Figure 17A. This implies that the length of the data sent is substantially longer than only the message itself and the tag as the length of the encrypted inner result must be about the same as the message itself (for otherwise function 1502 would not be reversible). Now when combining Carman and Graveman, there is essentially one option: take Carman and use Graveman instead of SHA-1 in 1506 (Figure 15). The alternative to use Carman in Graveman would be illogical and unworkable. Carman could be placed in front of Graveman but then the input to Graveman would be that tag, the message and the intermediate result. This would destroy the property of Graveman of being an AMAC as one bit change in the message will cause about half of the bits of the intermediate result to change and hence 1/4 of the input bits to Graveman will change which would then ruin the AMAC aspect of Graveman.

If one takes Carman and uses Graveman instead of SHA-1 in 1506 (Fig 15), the AMAC property of Graveman is destroyed as, as noted above, half the bits of the intermediate result will flip when changing one bit of the message. Hence one skilled in the art would *never* combine the two as to do so would add complexity without gaining anything and without obtaining the benefits of either.

Furthermore, the Carman construction, which relies heavily on the basic construct in Figure 15, is inefficient as a MAC code which is the sole purpose of the present invention. In Carman, the objective is to detect and correct errors and in doing so, many more bits must be sent than that only needed for MAC functions. Hence, one skilled in the art would *never* consider Carman as a MAC function itself. Further, as explained above, using Carman in Graveman destroys Graveman and therefore, one skilled in the art would never combine them.

The Examiner further rejected claims 5-6 under 35 U.S.C. § 103(a) as being unpatentable over Graveman and further in view of Carman *et al* and Shokrollahi (US 6,631,172). The Applicant respectfully traverse the rejection because, as noted above, it is technically impossible to combine Graveman and Carman to obtain the present invention. Because of this technical inability to combine the two, it would not have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Graveman with the teaching of Carman and Shokrollahi to authenticate the source and integrity of transmitted or stored information using a Reed-Solomon error correcting code wherein the tag value is determined by evaluating a Reed-Solomon encoding polynomial at a point determined by the key and the tag value is an element in a finite field.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



Michael Cameron
Registration No. 50,298

Date: April 11, 2008

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024
(972) 583-4145
michael.cameron@ericsson.com